P2000

Security Management System

software release notes

version 3.12 SP3

24-10685-149 Revision D
March, 2015

Johnson Controls

Copyright 2015
Johnson Controls, Inc.
All Rights Reserved

No part of this document may be reproduced without the prior permission of Johnson Controls, Inc.

If this document is translated from the original English version by Johnson Controls, Inc., all reasonable endeavors will be used to ensure the accuracy of translation. Johnson Controls, Inc. shall not be liable for any translation errors contained herein or for incidental or consequential damages in connection with the furnishing or use of this translated material.

Due to continuous development of our products, the information in this document is subject to change without notice. Johnson Controls, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with furnishing or use of this material. Contents of this publication may be preliminary and/or may be changed at any time without any obligation to notify anyone of such revision or change, and shall not be regarded as a warranty.

Other Manufacturers' Documentation

Johnson Controls does not duplicate documentation of other equipment manufacturers. When necessary, Johnson Controls provides documentation that supplements that of other manufacturers. When unpacking your equipment, keep all original manufacturer documentation for future reference.

Technical Support

Johnson Controls authorized dealer representatives can call the Field Support Center at (800) 524-1330 or (414) 524-5000 and use options 6, 1, 7. System users that need information on maintenance contracts or on-site field support can call a local Johnson Controls sales or service office.

Acknowledgment

Metasys® and Johnson Controls® are trademarks of Johnson Controls, Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

P2000 V3.12 SP3 SOFTWARE RELEASE NOTES

This document contains supplemental information pertaining to the following P2000 software releases:

- P2000 Version 3.12
- P2000 Version 3.12 Service Pack 1 (SP1)
- P2000 Version 3.12 Service Pack 2 (SP2)
- P2000 Version 3.12 Service Pack 2 (SP3)

The P2000 Version 3.12 SP3 software includes the **complete P2000 Version 3.12 software and Service Packs 1, 2, and 3**, with the recent bug fixes and software enhancements. The part number of the service pack is P2K-SW-312SP3.

NOTE: You can still use the G&D® (Giesecke and Devrient™) smart card encoder with P2000 V3.12 SP3, but it is no longer available for purchase.

INTRODUCTION

This document is divided into the following sections:

- P2000 V3.12 SP3 General Information on page 2
- Summary of Changes in P2000 V3.12 and Service Packs on page 7
- Problems Fixed in Version 3.12 and Service Packs on page 17

For installation or upgrade instructions, refer to the *P2000 Software Installation* manual.

NOTE: If you have an existing P2000 Express V3.11 system and want to upgrade to P2000 V3.12 SP3, you must first register your existing system with a full-version registration key for P2000 V3.11, and then follow the usual upgrade process. Refer to the *P2000 Software Installation* manual for more information on obtaining the registration key and upgrading your software.

Important Notes When Installing or Upgrading Software

For detailed information about server setup and subsequent installation of P2000 prerequisites and software, refer to the *P2000 Software Installation* manual.

P2000 and DVN Software Installation

When you install the P2000 and DVN software on the same machine, install SiteManager first. If you install the P2000 software first, and add SiteManager afterwards, re-install the P2000 software to ensure proper operation.

Registration of the P2000 Software and Options

All P2000 systems require a Registration Key. For upgrades, you need to enter the Registration Key *during* the upgrade procedure, so make sure to obtain it beforehand.

If your P2000 system includes options, you also need Option Keys.

For detailed information on how to obtain and use the Registration Key and Option Keys, refer to the *P2000 Software Installation* manual.

P2000 V3.12 SP3 General Information

This section describes P2000 V3.12 SP3 packages, options, and system configuration.

P2000 V3.12 SP3 Packages

The P2000 prerequisites contain Microsoft® SQL Server™ Express Edition and the majority of updates available from Microsoft at the time of the release. Newer updates may be available on the Internet at the time you perform the installation. We recommend that you use the latest updates available.

You use the same P2000 software DVD to install or to upgrade P2000 software on the server and on the workstations.

The following P2000 packages are available.

Table 1-1: P2000 Packages

	P2000 Server Package	P2000 Workstation Package	P2000 Software-Only Package	P2000 Software Upgrade Package
Server/Workstation Hardware	✓	✓		
Operating System Installed	✓	✓		
Database Engine Installed	✓	N/A		
P2000 Prerequisites and P2000 Software Installed	✓	✓		
P2000 Prerequisites and Software	✓	✓	✓	✓
P2000 User Documentation	✓	✓	✓	✓
P2000 Tutorial	✓	✓	✓	✓

P2000 Options

P2000 Version 3.12 SP3 offers the following options:

- Alarm Manager
- Archive Report Server
- Aritech Intrusion
- Assa Abloy® Panels
- Bosch® Intrusion
- Change Tracking (FDA)
- Cardkey™ Legacy Serial Panels
- Cardkey S321 Serial Panels
- Commend Intercom
- Digital Video Integration (for a list of supported DVM and DVR protocols refer to the *P2000 Digital Video Integration Manual*)
- Enterprise
- Fire Alarm Panel Interface
- HID® Controllers
- Isonas Controllers Pack 2
- OSI Panels (not supported on systems with Windows Server 2012 or SQL Server 2012)

- Mercury® panels
- Otis® Compass™ Elevator
- P900 Panels
- SIA Interface
- Zenitel Intercom

P2000 SMS Application Program Interface (API)

Various published P2000 SMS Application Program Interfaces (APIs) are available for third party integrations into the P2000 SMS. The APIs published by Johnson Controls are product features which are tested and validated, and customer issues related to their use can be resolved through HotFixes and Service Packs by raising cases through the appropriate support channels. Full technical support is available for tickets associated with a P2000 SMS APIs published by Johnson Controls.

IMPORTANT: Direct database manipulation may void all warranties, and may render the P2000 SMS unsupportable.

P2000 System Configuration

The P2000 Security Management System (SMS) operates in a client-server architecture. You must install P2000 software on the system server prior to installing it on the system workstation.

NOTE: Use a dedicated server for the P2000 SMS; that is, install only the Microsoft Windows® operating system, the SQL Server database engine, and the P2000 software. To install and run other third-party applications, please contact a Johnson Controls® Technical Support specialist for assistance.

This section lists and describes supported Windows operating system and SQL Server combinations for both standard and small P2000 systems.

A standard P2000 SMS includes more than 64 readers, 5,000 cardholders, and two workstations.

Table 1-2: Supported P2000 Server Configuration Options for a Standard P2000 SMS

	SQL Server 2012 Standard (32-bit)	SQL Server 2012 Standard (64-bit)	SQL Server 2008 R2 Standard (32-bit)	SQL Server 2008 R2 Enterprise (64-bit)
Windows Server® 2012 Standard	✓	✓[1]	✓	✓
Windows Server 2008 R2 Standard	✓	✓	✓	✓
Windows Server 2008 Standard and Standard without Hyper-V (32-bit)	✓		✓	
Windows Server 2008 Standard and Standard without Hyper-V (64-bit)	✓	✓	✓	✓

1. Recommended platform.

NOTE: Support for OSI panels requires IIS Version 6.0 or 7.0. Also, OSI panels are not supported on systems with Windows Server 2012 or SQL Server 2012.

NOTE: Some versions of Windows may require that you install a service pack before you install SQL Server. Refer to the Microsoft documentation for more information.

You can use SQL Express on a Windows server as the database for a *small* P2000 SMS; a small P2000 SMS supports fewer readers, cardholders, and workstations than a standard P2000 SMS.

Table 1-3: Supported P2000 Server Configuration Options for a Small P2000 SMS

	SQL Server 2012 Express (32-bit)	SQL Server 2012 Express (64-bit)	SQL Server 2008 R2 Express (32-bit)	SQL Server 2008 R2 Express (64-bit)	SQL Server 2008 R2 Express with Tools (32-bit)	SQL Server 2008 R2 Express with Tools (64-bit)	SQL Server 2008 R2 Express with Advanced Services (32-bit)	SQL Server 2008 R2 Express with Advanced Services (64-bit)
Windows Server® 2012 Standard		✓		✓		✓		✓
Windows Server 2008 R2 Standard		✓		✓		✓		✓
Windows Server 2008 Standard and Standard without Hyper-V (32-bit)	✓		✓[1]		✓		✓	
Windows Server 2008 Standard and Standard without Hyper-V (64-bit)		✓		✓		✓		✓

1. Recommended platform.

P2000 Workstations

We recommended the following minimum workstation specifications:

- Windows 8 or Windows 7
- 768 MB RAM
- 1024 x 768 resolution video card, 24-bit color
- 17-inch video monitor
- 120 GB hard drive
- 10/100BASE-T Network controller card
- DVD drive

Workstations do not require a SQL Server database. The following workstation operating systems are: supported

- Windows 8 (32-bit): Professional and Enterprise
- Windows 8 (64-bit): Professional and Enterprise
- Windows 7 (32-bit): Professional, Ultimate, and Enterprise
- Windows 7 (64-bit): Professional, Ultimate, and Enterprise

SUMMARY OF CHANGES IN P2000 V3.12 AND SERVICE PACKS

This section separately lists the changes for P2000 Version 3.12, P2000 Version 3.12 Service Pack 1, and P2000 Version 3.12 Service Pack 2.

Changes in Release 3.12

Release 3.12 includes the following new functionality:

- P2000 Web UI, which lets you to access some P2000 features using a Web browser
- P2000 Archive Report Server, which archives P2000 data on a standalone system and allows reports to be run against the data using the P2000 Web UI
- Import/Export Tool for CK721-A and S321-IP reader terminals
- Alarm Manager (using the P2000 Web UI)
- Support for User Authentication through Active Directory using a user's Windows group assignment

- Distributed mode of deployment, where P2000 services run on one machine (the P2000 application server) and the P2000 databases are hosted on another machine (the P2000 database server)
- Support for Mercury® panels CKM-EP1501, CKM-EP1502, and CKM-EP2500. See Resources for Mercury Devices on page 12.
- Support for Schlage® PIM400-1501 panel (Schlage PIM400 integrated with Mercury EP1501). See Resources for Mercury Devices on page 12.
- Support for the following digital video protocols:
  - Milestone Xprotect™ Corporate Version 5.0 or newer, MIP software development kit (SDK) Version 3.0a
  - Milestone Enterprise Version 8.0 or newer, MIP SDK 3.0a
  - Milestone Professional Version 8.0 or newer, MIP SDK 3.0a
  - Milestone Express Version 1.0 or newer, MIP SDK 3.0a

Contact Milestone for more information about their software versions.

- The P2000 Login window has changed slightly to increase security. Refer to Changes to P2000 Login on page 12 for more information.
- Support for Aztec 2D barcodes in Web Access. Contact Technical Support for configuration details.

Changes in Release 3.12 Service Pack 1

The following changes and improvements were introduced in Release 3.12 Service Pack 1:

- Modified message classes to ensure that *EmployeeID* is included in messages that contain cardholder information (DCS 20833).
- Modified Cabinet Config to prevent an error message when saving a new record (DCS 20840).
- Modified Web Access to provide support for displaying Aztec 2D barcodes (DCS 21071).
- Modified Assa Abloy Interface service to prevent queued downloads from being deleted when the DSR is offline (DCS 20854).
- Modified Kone IP Elevator Config to limit the access time to a maximum of 30 seconds (DCS 20864).
- Modified Kone IP Controller Config to allow elevator group address 1 to be used for Primary/Backup KGC (DCS 20865).

- Modified CK720 download logic to ensure that the correct controller ID is used for a Kone IP controller (DCS 20866).
- Modified all panel interface services to add the ability to set terminal status to down when their parent panel goes down. This is done to resolve an issue with the Metasys system interface (CR 53935).

Key	HKEY_LOCAL_MACHINE\Software\ Johnson Controls\Pegasys\P2000 CK720 Priority Service V2.1
Name	SetTermsDownWhenPanelDown
Type	DWORD
Value	0 = normal operation, 1 = set terminals down when panel goes down

- Added option for Bosch® Video Management System (VMS) with Cameo SDK (DCS 21072).
- Modified Pegasys application to prevent a database deadlock error that occurs rarely on Enterprise systems (DCS 20874).
- Modified common image load and save dialogs to remove PDF files, which are not supported (DCS 20870).
- Modified Assa Abloy Interface service to ensure that the proper list of doors is assigned access to badges (DCS 20879).
- Modified Assa Abloy Interface service to eliminate download of badges under some conditions (DCS 20880).
- Modified Assa Abloy Interface service to eliminate the need to download time zones before badges after clearing an Assa Abloy® Door Service Router (DSR) (DCS 20881).
- Modified Cardholder application to launch the Search windows significantly more quickly on systems with large numbers of companies or departments (DCS 21073).
- Modified User Defined Fields to not delete currently selected Choice from all cardholders when deleting a specific Choice from a Selection Choice list (DCS 20892).
- Added option for Aimetis Symphony™ VMS (DCS 21074).
- Modified User Defined Fields to properly update cardholders when editing or deleting a specific Choice from a Selection Choice list (DCS 20939, 20958).

- Modified Pelco Endura Interface service to resolve an alarm monitoring issue on 64-bit systems (DCS 20954).
- Modified badge download logic for CK72x panels to ensure that all access groups with terminals on the panel being downloaded are downloaded first (DCS 20951).
- Modified panel download logic, Add Visitor, Area Control, AutoBadge Number Management, Events, Guard Tour service, MIS Interface service, PNT Periodic service, RTL Route service, Smart Download, and Visitor Request Management service to handle a full 64-bit badge number (DCS 20943).
- Modified Badge and Cardholder to handle a full 64-bit badge number (DCS 20943).
- Modified OSI Integration service to work with the new Stanley® Wi-Q™ system and SDK (DCS 21075).
- Modified RTL Route Service to enhance error handling during host event processing (DCS 20972).
- Modified Web Badging to properly handle a badge that is not assigned a badge design (DCS 20983).
- Modified Events to ensure that a condition value is entered when the condition type is Badge or Cardholder (DCS 20898).
- Modified HID Interface service to ensure that badges are deleted from the controller under all conditions (DCS 20985).
- Modified Kone IP Elevator Config to limit the properly handled time zone selections (DCS 20987).
- Updated OnSSI Interface to support the OnSSI v3.6 SDK for Ocularis CS (DCS 21076).
- Updated Nextiva Interface to support the Nextiva v6.3 SDK (DCS 21077).
- Modified common database classes to properly handle an item name containing “where” (DCS 21023).
- Modified CK720Priority to solve a problem where it may not recover from an error under very rare conditions (DCS 21061).
- Modified panel interface services to solve a problem where they may stop working correctly under very rare conditions (DCS 21068).
- Modified Intrusion Interface service to solve a problem where the service would occasionally hang when reading data from a Bosch Intrusion panel (DCS 21067).

- Modified XmlRpc Interface service to correct operation of the DoorEnable method (DCS 21070).
- Modified Assa Abloy Interface service to ensure that time zones are correctly downloaded (DCS 20851).

Changes in Release 3.12 Service Pack 2

The following changes and improvements were introduced in Release 3.12 Service Pack 2:

- Added support for Dual Ethernet support in Mercury CKM-EP2500 panels.
- Added support for Anti-Passback and Entry-Exit logic in Mercury panels.
- Added support for "Snow emergency" feature in Mercury configuration.
- Added **Multi-Card Access Time Out** to Mercury Facility.
- Added **Door Open Warning Time** to Mercury terminal configuration.
- Added **Cardholder Shunt Override** to Mercury terminal configuration.
- Added support for Assa Abloy DSR Version 5.0 (support for prior versions of Assa Abloy DSR has been removed).
- Added support for Avigilon® Version 5.0 video management system (VMS).
- Added support for HID Edge EVO hardware (the extended functionality provided by the EVO version of HID Edge is not currently supported).
- Added support for 1024 Assa Abloy locks.

NOTE: For optimal system performance, we recommend you configure your system with few DSRs as possible; each DSR can connect with up to 1024 locks.

Changes to P2000 Login

The Login window has changed slightly in P2000 Version 3.12. You can no longer select a partition on the Login window. This change makes it harder for an attacker to gain unauthorized access to the P2000 system. This change has no effect on your login if you have login credentials for the SuperUser partition or if you are using your non-SuperUser login credentials to log in to a workstation that belongs to a partition assigned to you.

The only effect this change has is if you are using your non-SuperUser login credentials to log in to a workstation that does *not* belong to a partition assigned to you.

To allow operators to access a workstation that does not belong to a partition assigned to them, set that workstation as Public. Note that once a workstation is set as Public, all known P2000 operators can use that workstation to access the system.

Resources for Mercury Devices

The Mercury panel firmware upgrade files are located in:
C:\P2000 Resources\Mercury Resources\Firmware\

The MR51E and CKM-MR51E address tool is located in:
C:\P2000 Resources\Mercury Resources\MR51e Addressing Tool\

Run the firmware upgrade files from a local drive, not a network.

Changes in Release 3.12 Service Pack 3

The following enhancements to Assa Abloy support have been introduced in P2000 Software V3.12 SP3. See the referenced pages for details:

- Performance Optimizations for Assa Abloy Processes on page 13
- User Interface Changes to Streamline Reloading DSR on page 14
- Changes to Assa Abloy's Panel Time Zone Table on page 16
- Door Control and Output Control Performance Improvements on page 16
- Installer for DSR Version 5.0.4. (DCS 6649)

Performance Optimizations for Assa Abloy Processes

Enhancements to Assa Abloy support include Access Group Delete, Access Group Edit, and P2000 Assa Abloy Interface Service optimizations.

- Access Group Delete optimizations

  Prior to this optimization, all controller integrations without direct Access Group Support (for example, Assa Abloy) downloaded all badges in a system in order to process a delete request for an Access Group. With this optimization, downloads are now limited to only the badges affected by the deleted Access Group, subsequently improving the performance load generated by such actions.

- Access Group Edit optimizations:

  Prior to this optimization, an Access Group Edit in the P2000 system triggered a download of all affected badges for each Assa Abloy Lock (referred to as ‘panel” in the P2000 software). Following the optimization, there is a single download to the DSR for each badge effected by the edit, leveraging the DSR functionality of determining and managing access authorizations to all Assa Abloy Locks.

- P2000 Assa Abloy Interface Service optimizations for memory consumption

  The enhancements delivered in this version introduce optimizations for the memory consumption associated with the Assa Abloy DSR Interface Service. Prior to the optimization numerous tables were opened for each lock, and kept open for the lifetime of the service. Following the optimization, memory is cleaned up by releasing the tables after their use concludes.

User Interface Changes to Streamline Reloading DSR

Two new buttons in the Assa Abloy DSR Edit screen, **Quick Restore** and **Full Download**, streamline the reloading of DSR.

The **Quick Restore** button downloads the most important data to the DSR to get the system going again after a DSR was cleared. The **Full Download** button downloads complete provisioning data from the P2000 server.

This section describes in detail selected Assa Abloy procedures:

- How to use the new buttons, **Quick Restore** and **Full Download**, to clear and reload a single DSR or all DSRs.
- How to clear and reload one or more locks.

NOTE: If the DSR has gone through abnormal conditions that make its database inconsistent with the P2000 data, use the **Clear DSR** button. (After clearing the DSR of P2000 data, and once the DSR downloads these changes to the Assa Abloy locks, cardholders are unable to gain access.) Follow by reloading the DSR with the P2000 data.

To clear and reload a single DSR:

1. From the System Configuration window, select the DSR you wish to clear and reload and click **Edit**.
2. Click **Clear DSR**.
3. Click **Quick Restore**.
4. Click **Full Download**.
5. Click **OK** to close.

To clear and reload all DSRs:

1. From the System Configuration window, edit each of the DSRs you wish to clear and reload.
2. For each DSR, click **Clear DSR**.
3. Edit one DSR and click **Quick Restore** to download all DSRs with the most important data.

4. Edit one DSR and click **Full Download** to download all DSRs with all data.

5. Click **OK** to close.

To clear and reload a single lock:

1. From the System Configuration window, select the Assa Abloy panel you wish to clear and reload and click Edit.

2. Click **Clear Lock**. This deletes all P2000 data, such as badge data or access groups, from the Assa Abloy panel.

3. Click **OK** to close.

4. Open the Download application and select the Assa Abloy panel.

5. From the Item to Download box, select **Terminals** and **Badges**. Make sure that the **Delete Badges From Panel Before Download** flag is not selected; otherwise, the download process takes much longer.

6. Click **Download** to repopulate the lock with the P2000 data.

To clear and reload several locks:

1. From the System Configuration window, edit each of the Assa Abloy panels you wish to clear and reload.

2. For each panel click **Clear Lock**. This deletes all P2000 data, such as badge data or access groups, from each Assa Abloy panel.

3. Click **OK** to close.

4. Open the Download application and select all Assa Abloy panels that were cleared.

5. From the Item to Download box, select **Terminals** and **Badges**. Make sure that the **Delete Badges From Panel Before Download** flag is not selected; otherwise, the download process takes much longer.

6. Click **Download** to repopulate the locks with the P2000 data.

Changes to Assa Abloy's Panel Time Zone Table

You no longer have to list the time zone in the Assa Abloy's Panel Time Zone Table (except when you want it listed in the table to select for timezone override).

Each Assa Abloy lock can only store up to 32 different time blocks. A time zone may have multiple time blocks. We recommend that you keep the Time Zone strategy for Assa Abloy locks as simple as possible.

- Keep the number of time blocks inside each lock to a minimum (by using a very basic Time Zone strategy for Assa Abloy locks).
- The access rights of a badge are determined by the combination of Access Groups and Time Zones.
- Ensure that Access Groups containing Assa Abloy panels are only paired with Time Zones that are suitable for Assa Abloy panels.
- You do not have to list a Time Zone in the Panel Time Zone table of an Assa Abloy panel in order to use it to grant access to badges.
- You have to list a Time Zone in the Panel Time Zone table of an Assa Abloy panel in order to use it as the "Override Timezone" in the terminal definition.
- You cannot use the exclusion of a Time Zone from the Panel Time Zone table to curtail the access rights of defined badges. Instead, choose Access Groups to only include the applicable Assa Abloy panels.
- In general, we do not recommend removing or rearranging Time Zones in a Panel Time Zone table. If such actions are necessary, we recommend downloading all Time Zones and badges to the affected panel after you make the changes.
- We recommend that you select one Assa Abloy panel and list all time zones that are used on the DSRs in this panel's Panel Time Zone table. You can then select this panel in the Download application to download Time Zones, if necessary.

Door Control and Output Control Performance Improvements

Enhancements to Door Control and Output Control include:

- Performance improvements when you launch the application and load the lists of partitions and items to be controlled.
- Optimizations to loading user permissions.

PROBLEMS FIXED IN VERSION 3.12 AND SERVICE PACKS

The following issues have been solved in P2000 Software Version 3.12.

Problems Fixed in Version 3.12	
Badging	Modified badge download routines to allow certain optimizations to be disabled via the registry (DCS 20778). To disable the optimization and therefore work around the issue identified in the DCS, add the following registry key on the server and all workstations. This registry key should be entered only on systems which exhibit the issue described in the DCS: • Key HKEY_LOCAL_MACHINE\Software\Johnson Controls\Pegasys\P2000 CK720 Download Service • Name DisableOptimizedBadgeAGDownload • Type DWORD • Value 1
Cardholders	Modified Cardholder to prevent users with edit-only permissions from adding new Journal entries (DCS 20330).
	When you rename a UDF choice assigned to one or more cardholders, and select **<none>** as **New Choice**, then not just the renamed choice but *all* UDF choices under that UDF name, previously assigned to cardholders, get cleared (Defect #5928).
Elevators	Modified Elevator Configuration to display a warning message when terminals above index 16 are used (DCS 20706).
Enterprise	Modified the Enterprise merge script to properly handle multiple reports with the same name (DCS 20722).
HID	Modified the HID Interface service to correct a problem where the service may not recover after certain errors (DCS 20772).
	Modified the HID Interface service to provide basic support for two badge formats per reader (DCS 20786). To specify a second badge format for all readers, add the following registry key on the server: • Key HKEY_LOCAL_MACHINE\Software\Johnson Controls\Pegasys\P2000 HID Interface Service • Name SecondFormatFile • Type String • Value <complete path and file name of P2000 badge format file>
Cameras	Modified Event Edit to ensure the Camera Name shows in the event summary for actions of type Camera Preset (DCS 20815, 20817).
CK720	Modified the CK720 Download service to use a non-fixed initialization for encryption (DCS 20774). Note: CK72x controller firmware must also be updated when this patch is installed if encryption is enabled.

Problems Fixed in Version 3.12	
Elevator	Modified elevator database classes to prevent a database error when adding a new elevator on some systems (DCS 20840).
HID	Modified the HID Interface service to properly handle dates on systems with different date formats (DCS 20781).
Milestone	Modified the Milestone MIP Viewer to correct multiple user interface issues with the date and time (DCS 20805, 20807).
	Modified the Milestone MIP Viewer to correct controlling the PTZ from the live video screen (DCS 20816, 20819).
	Modified the Milestone MIP Viewer to properly export video after the date and time have been set manually (DCS 20795, 20813, 20829).
	Modified the Milestone MIP Interface service to properly handle messages from dry contacts (DCS 20797, 20811, 20822).
	Modified Milestone MIP data handling to ensure all cameras are reported when a list of cameras is requested (DCS 20799).
	Modified the Milestone MIP Viewer to add tooltips to control buttons (DCS 20803, 20809).
	Modified the Milestone MIP Viewer to display all available thumbnails when changing to Browse mode (DCS 20796, 20804, 20808, 20814).
	Modified the Milestone MIP Viewer to prevent an exception message when switching to a full screen view (DCS 20812).
	Modified the AV Service and Milestone MIP Interface service to correct a problem where the P2000 stops receiving camera motion detection alarms (DCS 20832).
	Modified the Milestone MIP Viewer to correct time display issues (DCS 20834, 20841, 20844).
	Modified the Milestone MIP Interface service to properly handle **DVR disconnected** messages (DCS 20843).
P2000 Express	Modified database classes to correct services to starting on P2000 Express installs (DCS 20787).
Periodic Service	Modified database classes to prevent an error in Periodic Service when checking for free disk space (DCS 20802).
Real Time List	Modified the Real Time List to activate popup menu on AV Dry Contact alarms (DCS 20842, 20845).
S321IP	Modified the S321IP Interface service to correct a problem where the service may not recover after certain errors (DCS 20773).

The following issues have been solved in P2000 Software Version 3.12 SP1.

	Problems Fixed in Version 3.12 SP1
Alarms	The Alarm Response text application crashes when user clicks the **Text** column in the Alarm Response Text window. (Defect #5685)
Cardholder Definition	A UDF choice value assigned to one or more cardholders is deleted from all cardholders when you edit and then cancel a choice value for the associated UDF. (Defect #5763)
CK7xx Controllers	CK7xx controllers cannot connect to a P2000 Server when the FDA Part 11 feature is enabled. (Defect #3324)
Database Maintenance and Validating Digital Signatures	The digital signatures of some database tables are incorrectly reported as failing during system validation. (Defect #3249)
DVR/VMS: Bosch	After installing a Bosch DVR, the following message appears in the RTL: “Bosch Interface Service not configured to start.” (Defect #5684)
DVR/VMS: Milestone	When a Milestone MIP switch is configured, no record of the switch being configured is stored in the AVPreset_save table. (Defect #3276)
DVR/VMS: Pelco Endura	When viewing two cameras in multiple panes view, the playback function does not work for the second camera. (Defect #5857)
Mercury Intrusion	Alarm generated while system is disarmed changes to “Armed/ Alarmed” in the P2000 system. (Defect #5683)
P2000 Software Upgrade	Upgrade to P2000 Version 3.12 generates an error message. (Defect #5923)
Panel Configuration	You cannot edit the S321-IP terminal name. (Defect #5865)
Panel Configuration: Kone IP Controller	When a Kone IP controller is created and then deleted in P2000, the delete record is not downloaded to the panel. (Defect #5648)
Reports	When you run a P2000 report in Arabic, Crystal Reports does not display P2000 data. (Defect #5646)
System Status	System Status shows that Mercury panel is up even when the Mercury Service is stopped. (Defect #5764)
S321-IP	S321 IP panel goes up and down when configured in P2000 SMS with the FDA option enabled. (Defect #5662)
XML-RMS Real Time Data Message	The XML-RMS Real Time Data Message for History Type 35 (Invalid Reader) omits the CardholderID. (Defect #5765)

The following issues have been solved in P2000 Software Version 3.12 SP2.

	Problems Fixed in Version 3.12 SP2
Alarm Categories	**Description:** Deleting Alarm Categories produces database errors, then stops functioning. (Defect #5741)
Aritech Panels	**Description:** An “Invalid Function Delete” message appears on the screen when you attempt to delete an Aritech Intrusion device. (Defect #5775)
Assa Abloy	**Description:** Access continues to be granted after removing access rights and executive privilege. (Defect #5962)
Database Maintenance and Validating Digital Signatures	**Description:** Clicking **Cancel** during the Validate Digital Signature function causes the Database Maintenance application to stop working. (Defect #3342)
DVR/VMS: Bosch Cameo	**Description:** The “AV Input Point to Camera” report does not display any records. (Defect #5771)
	Description: Software installation for displays incorrect path and file name Bosch Cameo components: **CameoSDKSetup.exe** and “C:\Program Files (x86)\Johnson Controls\P2000\AV\Bosch\Bosch Cameo SDK Installer.”
	The correct path and file name are as follows: **CameoSdk.msi** and “C:\Program Files (x86)\Johnson Controls\P2000\AV\Bosch\Bosch Cameo SDK Installer\CameoSdk.” (Defect #5926)
DVR/VMS: Pelco Endura	**Description**: After the camera’s preset is deleted from the AV Configuration, it can still be controlled from the **PTZ** tab in AV Player. (Defect #5817)
	Description: After the camera controls **Tilt**, **Pan**, and **Zoom** are disabled in the AV Configuration, they can be still used in the AV Player to control the camera. (Defect #5818)
	Description: The viewer application may fail to play live video. (Defect #5641)
DVR/VMS: Pelco X-Portal DX8100	**Description:** Multiple **Motion** and **Video Loss** alarms are triggered, and subsequent events occur (if defined), because **Alarm Debounce** values are ignored. (Defect #5620)
Foreign Language Pack	**Description:** When computer language is set to German, P2000 Tutorial fails to launch. (Defect #6017)
HID Edge	**Description:** When you add “Second Badge Format File” into the Registry Editor and download the second card format, an error host event message is sent to the RTL. (Defect #5738)
Mercury® Controllers (CKM-EP1501, CKM-EP1502, CKM-EP2500, as well as EP1501, EP1502, EP2500)	**Description:** A door contact does not report correctly when it is associated with the input calibration table. (Defect #5745)
	Description: When you un-bypass an active zone that was bypassed before, alarms are not generated when an area is armed. (Defect #3128)

	Problems Fixed in Version 3.12 SP2
OSI	**Description:** When an OSI terminal time zone is in an inactive state, but the time zone for **PIN Required** is active, the OSI terminal grants access to a valid cardholder. (Defect #6146)
	Description: When OSI Facility Access Groups are used, the OSI Facility data may not be downloaded correctly and all further OSI downloads may be blocked. (Defect #6142)
P2000 Alarms	**Description:** Deleting Alarm Response text generates a “Violation of Unique Key constraint” error. (Defect #5737)
P2000 Database	**Description:** On P2000 systems with the FDA option enabled, a database error is generated when you edit UDF selection two times. (Defect #5803)
P2000 Software Installation	**Description:** When you install P2000 software on a system that is running Windows Server 2012 (64-bit), error messages about setting IIS ISAPI restrictions appear. After closing them, you can proceed with the installation. (Defect #4402)
Partitions	**Description:** Adding P2000 partitions with the same name generates an error, as designed. However, if you subsequently try to add a partition with a unique and valid name, “Operation failed” error is generated. (Defect #5773)
Web Access	**Description:** Web Access does not work on computers using Windows Server 2012. (Defect #4403)

The following issues have been solved in P2000 Software Version 3.12 SP3.

	Problems Fixed in Version 3.12 SP3
Assa Abloy	**Description:** Restart of the P2000 Assa Abloy DSR Interface Service is required after changing Special Access Flags, but there is no information prompting the user to do so. The following needs to be displayed: “Changing any Flag assignment will require a restart of the P2000 Assa Abloy DSR Interface Service” and “Changing any Assa Abloy Facility data will require a manually initiated download of all badges to the DSR.” (Defect #10536)
	Description: When a badge is added to Assa Abloy panels that has only an end date but no start date, the end date is not effective until the badge is downloaded to the panel a second time. (Defect #7919)
	Description: Assa Abloy door status stays in “Forced Open” until the next door transition occurs. (Defect #7204)
	Description: Presenting a badge that is not known to an Assa Abloy panel should result in an “Invalid Card” access decision, not “Invalid Reader.” (Defect #6761)
	Description: When replacing doors in an access group the change does not become effective if the number of doors is the same before and after the change. (Defect #9070)
Access Groups	**Description:** Deleting Access Groups needs to be optimized by storing Affected Badges. (Defect #7940)
OPC Intrusion	**Description:** OPCSubscription.exe memory consumption grows in an unchecked manner. (Defect #7961)
S321-IP	**Description:** Badges associated to the Access Group of S321-IP terminals continue to grant access after Access Group is deleted. (Defect #10621)
XML-RPC	**Description:** An error occurs in P2000-XMLRPC Exerciser. (Defect #6510)

LIMITATIONS AND KNOWN PROBLEMS IN VERSION 3.12 AND SERVICE PACKS

The following issues have been reported in P2000 Software Version 3.12 and Service Packs 1, 2, and 3. They may be addressed in a subsequent release of the software.

	Limitations and Known Problems
Access Group Application	**Description:** The Details tab in the Access Group application displays Mercury terminals that are defined in the General tab, and also Mercury terminals that are assigned to elevators included in the Floor Groups defined in the Elevator tab. (Defect #3305, #2695) **Workaround:** None.
Alarm Manager (P2000 Web UI)	**Description:** When a service pack or patch update from Microsoft adds new time zones to the Windows operating system, the Alarm Manager time zone list displays the new time zones in the language selected on the server where the P2000 Web UI is installed, instead of the language chosen by the user in their browser language settings. **Workaround:** None.
	Description: A defect in Microsoft IIS 7.0 and 7.5 software may result in the P2000 Web UI being inaccessible to users with 32-bit web browsers. Users see an HTTP 403 error message and are unable to view the P2000 Web UI. (Defect #2273) **Workaround:** Apply the following hotfix from Microsoft: support.microsoft.com/kb/980368
Alarm User Interfaces (Alarm Manager on P2000 Web UI and Alarm Monitor on P2000 workstation)	**Description:** When you apply the operator name, filter alarm updates may become invisible to other operators, but the alarm is not removed from Alarm Manager or Alarm Monitor until you refresh the screen. (Defect #2798) **Workaround:** Refresh the screen.
	Description: Under certain circumstances, an alarm that should only be seen by one operator (because a message filter is in place) may be visible to a second operator until the screen of the second operator is refreshed. This is caused by a defect in the data service that supplies data to both alarm user interfaces. (Defect #2337) **Workaround:** Refresh the screen.

	Limitations and Known Problems
Aritech Panels	**Description:** Aritech intrusion Areas, Zones and Annunciators fail to download to the P2000 server after restarting the OPC service. (Defect #3080) **Workaround:** If “The Launching User**”** setting does not work, change it to “The Interactive User” and restart the P2000.
	Description: On systems using Windows Server 2012 and SQL Server 2012, Aritech intrusion Areas, Zones and Annunciators fail to download to the P2000 server after restarting the OPC service. (Defect #5767) **Workaround:** None.
Assa Abloy®	**Description:** An error message occurs in System Configuration when you try to delete a time zone used by Assa Abloy panels. (Defect #6767) **Workaround:** This error message indicates that the P2000 Assa Abloy DSR Interface service has not yet forwarded the deletion information to the DSR. Wait for the information to get forwarded, and then delete the time zone.
	Description: When you delete a DSR that is still connected to the P2000 server, it may bring panels back to the P2000 server that are in the process of being deleted. (Defect #6768) **Workaround:** Disconnect the DSR from the P2000 server before deleting it.
	Description: Errors related to the Assa Abloy DSR interface appear in the Real Time List when you try to perform a Download. (Defect #6775) **Workaround:** Avoid unnecessary downloads using the Download application or through Download event actions. We recommend that you leave the “Delete Badges From Panel Before Download” flag unchecked when downloading badges to multiple locks on a DSR. Otherwise, the DSR may be tied up in a large amount of internal data processing and may not respond in time to requests made by the P2000. Refer to the *P2000 Software User* Manual for detailed recommendations.
	Description: Automatic Download does not work when you add all Time Zones to all Assa Abloy panels. (Defect #6764) **Workaround:** When integrating with a large number of Assa Abloy locks, configure the P2000 system’s SQL server **Maximum server memory (in MB)** setting to leave 2 GB for the rest of the system. That is, when the system has 8192 MB of RAM, 2048 MB must be reserved for the rest of the system, and 6144 MB may be used by SQL server.

	Limitations and Known Problems
Assa Abloy® (continued)	**Description:** Badges with Executive privilege are counted in the Lock Details tab when downloaded to an Assa Abloy DSR. However, due to errors in the DSR Support Tool, they do not appear on the Users in Lock tab. (Defect #10284) **Workaround:** None.
	Description: Foreign Key Constraint errors are displayed when you try to delete the DSR from P2000 after restoring the DSR database on DSR machine. (Defect #10578) **Workaround:** If the DSR has gone through abnormal conditions that make its database inconsistent with the P2000 data, clear and reload the DSR. See User Interface Changes to Streamline Reloading DSR on page 14.
	Description: Internet Explorer 11 is not supported by Assa Abloy DSR Support Tool. (Defect #6233) **Workaround:** None.
	Description: Help on the DSR support tool does not work. (Defect #9989) **Workaround:** None.
	Description: Upgrade from DSR 5.0.2 to DSR 5.0.4 occasionally may fail. (Defect #9983) **Workaround:** End the failed installation process and follow this upgrade outline: 1. Uninstall the DSR, but, when asked, select to leave the DSR database in place. 2. Uninstall all versions of Java. 3. Delete the directory where the DSR was installed (usually C:\Program Files\DSR). 4. Install DSR 5.0.4, and when asked, select to use the existing database.
Assa Abloy Aperio™ Devices and Mercury Integration	**Description:** Doors connected to Aperio device cannot be unlocked from the P2000 using the Main menu's Control All Doors command, from the Real Time Map, or from the Door Control window. Even though the option to unlock them is displayed, unlocking Aperio doors from these applications is not supported. (Defect #4352) **Workaround:** None.
	Description: Mercury door control procedures and triggers do not work with Aperio wireless locks. (Defect #6393) **Workaround:** None.

Limitations and Known Problems	
Assa Abloy Aperio™ Devices and Mercury Integration (continued)	**Description:** On the EP2500 panel with the Aperio terminal reader configured for Card and Pin Required, no access is granted after presenting a valid badge and PIN code. (Defect #6587) **Workaround:** After presenting the badge, there is a 2-3 second window in which the A100 lock does not accept any key presses. As a general recommendation, wait until you see the red LED light up before entering PIN. In “PIN before Badge” mode, wait to present your badge until the red LED has flashed 3 times after you enter your PIN followed by the # sign. This also takes about 2-3 seconds. Also, some locks require that you enter the asterisk key (*) key after the PIN code instead of the pound key (#).
	Description: Mercury “Door Override” feature is not available for Aperio locks. It is also not available at the door, that is, the door cannot be overridden by keying in a number of minutes.(Defect #6529) **Workaround:** None.
Badge Number	**Description:** When you try to edit badge number, an error message appears. This happens on systems with one or more Mercury panels. (Defect #6739) **Workaround:** Create a new badge with the new number and delete the old badge.
Badge Resync	**Description:** When you run Badge Resync with **Select All** option enabled, messages about the badge resync do not appear in the Real Time List. (Defect #6287) **Workaround:** None.
Bosch Intrusion	**Description:** Bosch Intrusion Area Alarms will re-alarm if left in the Alarm Monitor window when the intrusion system is armed or disarmed. This effectively results in a false alarm caused by the arming or disarming of the area. (Defect #6731) **Workaround:** Remove alarms from the Alarm Monitor window so they do not re-alarm when the intrusion system is armed or disarmed. (When you acknowledge alarms or remove them from the Alarm Monitor window, alarms do not re-alarm when the intrusion system is armed or disarmed.)
	Description: Intrusion Area alarms always display Alarm State “Normal.” (Defect #6732) **Workaround:** Before you configure your Bosch intrusion panels, ensure the correct settings are in place to establish communications between the P2000 server and the Bosch intrusion panel. We recommend the point response type for immediate response to be **0** for non 24-hour points, and **0** or **2** for 24-hour points.

Limitations and Known Problems	
CK720 Controller	**Description:** During stress testing of Central Grant Messages, a high amount of CK720 Priority Error Messages appears in the Event log, at a pace averaging about one every 3 minutes over a period of 12 hours. (Defect #5649) **Workaround:** None.
CK721-A Controllers	**Description:** After Badge changes, download is delayed and a corresponding message appears in the Real Time List. (Defect #12581) **Workaround:** None.
Database Backup and Restore	**Description:** P2000 software upgrade or database restore fail due to missing “esp_parameters table” columns in the P2000 database V3.12 and above. (Defect #15034) **Workaround:** This is a workaround for issues with P2000 database restore. For details on P2000 software upgrade workaround for the same bug, see this defect under P2000 Software Upgrade on page 35. Perform the following steps for each archived backup that needs to be restored for reports: 1. Restore the archive database to PegasysArchive without the “convert” flag enabled. 2. In the SQL Management Studio open the Pegasys database. 3. Delete the table "esp_parameters_save." 4. Open an Explorer window and navigate to: Program Files >Johnson Controls>P2000>sql. 5. In the sql folder, locate and double-click the script "Cr_enterprise_site_parameters_save.sql" to open it in a SQL Query window. 6. Execute the script to recreate the table. 7. Back up the PegasysArchive database in SQL to save for the next report needed. (The P2000 backup utility does not have this option). 8. Run a report against the fixed database. This will automatically start the convert utility.

Limitations and Known Problems	
DVR/VMS	**Description:** Moving between the **Search** and **Camera** tabs in the AVPlayer causes the AVPlayer to crash. (Defect #5617) **Workaround:** None.
	Description: The supported nudge factor range for all cameras supported by the P2000 is 1 to 100. The documentation incorrectly states the range as 1 to 255. (Defect #1988) **Workaround:** None.
	Description: Deleting the AV Switch fails because of a reference conflict in the Alarm Options table. (Defect #6216) **Workaround:** Before you can delete the AV Switch, you must delete all cameras in that AV Switch.Then you can delete the AV Switch itself.
DVR/VMS: Aimetis	**Description:** In live view, the viewer application shows an artifact in form of a black spot. (Defect #5753) **Workaround:** None.
	Description: When an invalid user ID or password is entered in the P2000 system, no login error message is displayed to the user. (Defect #5750) **Workaround:** Monitor the Real Time List for login errors.
DVR/VMS: Bosch Cameo	**Description:** A camera network connection failure or a camera power failure can cause the P2000 Bosch Viewer displaying that camera to stop working. (Defect #6131) **Workaround:** Close the program and re-open the viewer application. Until the camera is reconnected, the video display will be a blank screen for that camera.
	Description: Live video cannot be viewed when the Bosch VMS server and cameras are not on the local network. (Defect #6067) **Workaround:** Make sure the Bosch VMS server and cameras are on the same subnet as the P2000 server and workstations.
DVR/VMS: DVN 5000	**Description:** To integrate P2000 with the DVN 5000 Version 2.9 or Version 2.10, use the DVN Version 2.10 SDK. (Defect #1578) **Workaround:** None.

Limitations and Known Problems	
DVR/VMS: Nextiva	**Description**: When the Nextiva system is shut down or restarting, the AV Player crashes when you try to access a camera (instead of displaying a message that a camera image is not available). (Defect #5900) **Workaround:** None.
	Description: When you try to access stored video from the Real Time List or from the Alarm Manager, live video is displayed instead. (Defect #5901) **Workaround:** None.
	Description: When you right-click on an alarm and select **Display Map** in the Real Time List or in the Alarm Manager, a "No map available" message appears. (Defect #5902) **Workaround:** None.
	Description: When you manually stop recording, the system takes about a minute to respond. (Defect #5903) **Workaround:** None.
	Description: When you create an invalid preset and then try to use it, an error message does not appear like it should. (Defect #5898) **Workaround:** None.
	Description: When a P2000 event occurs, the Nextiva camera action works properly, but is not logged in the Real Time List. (Defect #5899) **Workaround:** None.
	Description: When you are viewing a video from a valid camera in the AV Player, and then select an invalid camera, the video from the valid camera continues to be displayed with the invalid camera's name in the title bar. (Defect #5904) **Workaround:** None.
	Description: P2000 event actions **Camera Send Alarm**, **Camera Send Alarm Associated Input**, and **Camera Send Alarm Associated Terminal** are not working properly. (Defect #6018) **Workaround:** None.

Limitations and Known Problems	
DVR/VMS: OnSSI	**Description**: The **Export Video** feature does not work on systems using Windows Server 2012. (Defect #5690) **Workaround:** Manually download and install needed codecs, for example, DivX, Xvid, or Mpeg4. We recommend Windows 7 Codec Pack Version 4.0.8.
	Description: "AV Input Point to Camera'" report does not display any record of a mapped input point. (Defect #6106) **Workaround:** None.
DVR/VMS: Panasonic® WJ-ND300 and WJ-ND400	**Description:** Playback functions **Rewind** and **Fast Forward** do not work correctly in the viewer application. (Defect #5634) **Workaround:** None.
Digital Video Integration: Pelco Endura	**Description**: Selecting cameras in a multiple panes view may crash the viewer application. (Defect #5640) **Workaround:** None.
	Description: When you disable only one function (Pan) of the PTZ control, all the PTZ functions (Pan, Tilt, and Zoom) as well as Focus and Preset buttons disappear from the video viewer. (Defect #6425) **Workaround:** None.
	Description: You cannot control the Zoom function directly from the video screen. (Defect #6428) **Workaround:** None.
	Description: You cannot take a snapshot and export a still image when playback is paused. (Defect #6437) **Workaround:** None.
Foreign Language Pack	**Description:** XML-RPC services do not encode high ASCII or multi-byte characters correctly. As a result, when the P2000 server generates an alarm in German, the P2000 Web UI Alarm Manager application displays the alarm initially, but when you navigate to a different UI page and then back to the Alarm Manager, the alarm does not appear. (Defect #6020) **Workaround:** None.
	Description: XML-RPC services do not encode high ASCII or multi-byte characters correctly. As a result, login to P2000 Web UI fails when language is set to Turkish, Chinese, Arabic, or Russian. (Defects #6062, #6101, #6091, and #6120) **Workaround:** None.

Limitations and Known Problems	
HID Edge	**Description:** The Door Control's **Return To Normal** command fails to control the HID terminal reader. (Defect #5742) **Workaround:** None.
HID Edge EVO	**Description:** The extended functionality provided by the EVO version of HID Edge is not currently supported. (Defect #6441) **Workaround:** None.
HID Edge EVO and ELM	**Description:** The Door Strike LED on the ELM lock module behaves differently from the LED on EDWM-M door and reader module. The Door Strike LED from the ELM lock module connected to EHRP40 reader always turns on. The Door Strike LEDs connected to the LED on EDWM-M door and reader module turn on only when the door opens and access is granted. (Defect #6603) **Workaround:** In order to change behavior of the ELM lock module from magnetic lock to electronic and vice versa, you have to change the EEPROM value. *P2000 V3.12 SP2 does not have this ability, therefore ELM lock module is currently not supported.*
Mercury® Controllers: CKM-EP1501, CKM-EP1502, CKM-EP2500, as well as EP1501, EP1502, EP2500	**Description:** If a panel tamper alarm is secured while the panel is powered down, the panel remains in the alarm state. (Defect #2729) **Workaround:** Open and close the panel enclosure while the panel is powered up and online.
	Description: Mercury integration with Schlage devices does not support assisted access time required by ADA (Americans with Disabilities Act). (Defect #5884) **Workaround:** Assisted access time is supported in Mercury Firmware Version 1.18.7 integration with Schlage devices.
	Description: CKM-EP2500 controller intermittently disconnects from the P2000 server for approximately 1 minute before reconnecting. (Defect #6224) **Workaround:** This issue occurs in CKM-EP2500 Firmware Version 1.17.3. Use Mercury Firmware Version 1.18.7 to avoid this problem.
	Description: 4-state REX inputs on Mercury controllers do not report the Open and Short condition to the P2000. However, since the door unlocks only when the REX is correctly activated, the Open and Short conditions cannot be used to unlock the door. (Defect #5932) **Workaround:** None.

Limitations and Known Problems	
Mercury® Controllers: CKM-EP1501, CKM-EP1502, CKM-EP2500, as well as EP1501, EP1502, EP2500 (continued)	**Description:** When using Mercury Firmware Version 1.18.7, an "Unknown User Command" warning message is generated any time you click **Apply** in the Intrusion Area Edit window. (Defect #6531) **Workaround:** None.
	Description: After upgrading panel firmware to V1.18.0, Mercury Configuration Manager does not display Timezone information for the controller (this defect does not apply to CKM-EP1501 and EP1501). (Defect #15086) **Workaround:** None.
	Description: After upgrading panel firmware to V1.18.0.371, Mercury Configuration Manager display of Timezone information is inconsistent (this defect applies only to CKM-EP1501 and EP1501). (Defect #15089) **Workaround:** None.
Mercury Controllers and PIN Duress Mode	**Description:** PIN Append is ignored when used with Mercury controllers in cases where the PIN is set for maximum digits and the badge is swiped before the PIN is entered; the PIN is accepted by the Mercury Controller before the duress code is processed. (Defect #3217) **Workaround:** If you want to use PIN Append (defined in the Mercury Facility application), select the Allow PIN before Badge option (defined in the Mercury Terminal application). The duress code will then be processed when users enter the PIN code before swiping the badge. You can also use Mercury Legacy Mode or PIN Code Offset.
Metasys Integration	**Description:** Metasys integration fails on a system using SQL Server 2012 Express Edition (32-bit). (Defect #3381) **Workaround:** None.
	Description: When the P2000 SMS is integrated with Metasys Version 6.1 or Version 6.5, the Metasys ADS hierarchy does not display red cross mark for disconnected CK721 or S321-IP controllers in the P2000 virtual machine. (Defect #5954) **Workaround:** None.

	Limitations and Known Problems
Milestone	**Description:** Milestone Corporate Dry Contacts Input does not report to the Real Time List after being triggered by a Panasonic NS202PTZ camera input. (Defect #2321) **Workaround:** None.
	Description: Camera Send Alarm actions (Camera Send Alarm, Camera Send Alarm Associated Input, and Camera Send Alarm Associated Terminal) are not supported when using Milestone protocol. (Defect #8961) **Workaround:** None.
MSEA	**Description:** The Pin Code Retry and Duress alarm does not return to secure in the ADS event view. (Defect #2323) **Workaround:** None.
	Description: Alarms are likely to be displayed out of order when, for the same alarm, multiple state transitions occurs within the same second. (Defect #5990) **Workaround:** None.
OSI	**Description:** Download queue gets jammed. (Defect #5743) **Workaround:** Add the following registry key on the server: • Key HKEY_LOCAL_MACHINE\Software\Johnson Controls\Pegasys\P2000 OSI Interface Service • Name DeleteErrorSpecialHandling • Type DWORD • Value 1
	Description: Download fails after you reduce **PIN Length** value in the OSI Facility Edit window. (Defect #5819) **Workaround:** None.
	Description: Certain types of messages about low battery are not being generated in the OSI system. Also, some low battery messages generated in the OSI system are not displayed in the P2000 Alarm Monitor. (Defect #5969) **Workaround:** None.
	Description: When a reader is deleted in the P2000 system, the following error is generated by the OSI interface: “RemoveReader failed - New transaction is not allowed because there are other threads running in the session.” (Defect #6079) **Workaround:** None.

Limitations and Known Problems	
Otis Elevator	**Description:** The P2000 SMS does not currently support the following: • Negative floors and floor zero • Rear doors (P2000 SMS does not differentiate between front and rear doors, and always gives access to both doors) • Otis “Segmentation” feature (used to keep people from different groups from riding together in an elevator) • Multiple Compass systems per P2000 SMS Also, during and after a power failure, the P2000 SMS and Otis Elevators behave inconsistently unless both systems are protected by an uninterruptible power supply. (Defect #6824) **Workaround:** No workaround is available for current limitations. For consistent performance during and after power failure, use an uninterruptible power supply.
P2000 Prerequisites Installation	**Description:** When you install P2000 prerequisites on a system that is running Windows 8, the installer detects that .Net Framework 3.5.1 SP1 is needed. It then attempts to install it from the Internet. If the Internet is not available, .Net Framework does not get installed. (Defect #6203) **Workaround:** Once the Internet connection is reestablished, use the Microsoft “Turn Windows features on or off” utility to turn on **.Net Framework 3.5 (includes .NET 2.0 and 3.0)**.
	Description: P2000 Prerequisite installation detects when ASP.NET MVC4 is needed on Web Server, but fails to install it. (Defect #6239) **Workaround:** Install Windows Powershell from Windows Server Manager and then run the P2000 Prerequisites again.
P2000 Software Installer	**Description:** Some files from the P2000 V3.12 SP2 installer display incorrect file and product versions. (Defect #12275) **Workaround:** None.

Limitations and Known Problems	
P2000 Software Upgrade	**Description:** Auto-update of a P2000 workstation fails. (Defect #5757) **Workaround:** Install P2000 V3.12 SP1 software on the workstation directly from the P2000 Installation DVD.
	Description: When you upgrade from P2000 V3.10 or earlier, with the intrusion feature configured, and then try to run OPC simulator, errors appear in the Real Time List. (Defect #10640, Defect #10732) **Workaround:** Verify that there is no duplication of intru_name and site combination in the intrusion_entity table. You can use the following script in SQL Server management Studio to find the duplicated records: SELECT intr_name, site, COUNT(*) FROM intrusion_entity GROUP BY intr_name, site HAVING COUNT(*) > 1
	Description: P2000 software upgrade or database restore fail due to missing “esp_parameters table” columns in the P2000 database V3.12 and above. (Defect #15034) **Workaround:** This is a workaround for issues with P2000 software upgrade to V3.12 and above. For details on database restore workaround for the same bug, see this defect under Database Backup and Restore on page 27. 1. If an upgrade failure occurred, restore the “old” database to be upgraded. 2. In the SQL Management Studio open the Pegasys database. 3. Delete the table "esp_parameters_save." 4. Open an Explorer window and navigate to: Program Files >Johnson Controls>P2000>sql. 5. In the sql folder, locate and double-click the script "Cr_enterprise_site_parameters_save.sql" to open it in a SQL Query window. 6. Execute the script to create the table and columns. 7. Refresh the database and verify the five “upd” columns are in the table. 8. Re-install the P2000 software V3.12 or above to complete the upgrade and conversion process.
Real Time Map	**Description:** Real Time Map Displays the Incorrect State of the Door During a Forced Door Condition. (Defect #10138) **Workaround:** None.

Limitations and Known Problems	
S321-IP Panel Download	**Description:** Some versions of Windows have a feature called Data Center TCP (DCTCP) that utilizes Explicit Congestion Notification (ECN) to enhance the TCP congestion control algorithm. When enabled (for example, in Windows 2012), the ECN considerably slows down the **"**Download to Panel" process. The download may take more than 20 minutes. (Defect #5689) **Workaround:** Disable ECN by running the following command from the command prompt: `netsh interface tcp set global ecncapability=disabled`
Schlage AD400 locks	**Description:** "Open for Access Time" cannot be used for AD400 locks. (Defect #6280) **Workaround:** None.
Stanley Wi-Q	**Description:** Stanley Wi-Q SDK Version 3.1.2 is not supported. (Defect #6851) **Workaround:** None.
Web Access	**Description:** You cannot print badge from Web Access. (Defect #5762) **Workaround:** In the Windows Internet Explorer®, add the P2000 server computer name or IP address to the list of trusted sites.
Web UI	**Description:** An "Unknown error" message occurs when you attempt to sign in to the P2000 directly from the web server (using "localhost") or connecting to the web server from a client. (Defect #5870) **Workaround:** One of the following solutions allow you to log in. • Enable **Allow Any IP Address** in the Edit SIte Parameters window. • If you do not want to allow any IP address, enter the IP address or computer name of the web server using the "External IPs" application (under Site Parameters). You must also select **Use for XmlRpc** in the External IP Edit window.
	Description: On servers using Windows Server 2008 SP2 32-bit operating system, when you attempt to access the P2000 Web UI via a front-end web server, an "HTTP 403 Forbidden" error message may occur. (Defect #6267) **Workaround:** None.

Security Solutions
(805) 522-5555
www.johnsoncontrols.com

We welcome your comments at BE-techpubs-security@jci.com.